

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

January 30, 1991

FIRMR BULLETIN B-1

TO: Heads of Federal agencies
SUBJECT: Electronic records management

1. Purpose. This bulletin provides guidance related to the creation, maintenance, use, and disposition of electronic records.
2. Expiration date. This bulletin contains information of a continuing nature and will remain in effect until canceled.
3. Contents.

Topic	Paragraph
Related material.....	4
Information and assistance.....	5
Definitions.....	6
Acronyms.....	7
Agency responsibilities.....	8
Creation and use of data files.....	9
Creation and use of text documents.....	10
Judicial use of electronic records.....	11
Security of electronic records.....	12
Selection and maintenance of electronic records storage media.....	13
Retention of electronic records.....	14
Destruction of electronic records.....	15
Comparison of Various Media For Information Storage and Retrieval.....	Attachment A

4. Related material.
 - a. 44 U.S.C. chapters 21, 29, 31, 33, and 35
 - b. FIRMR Subchapter B
 - c. 36 CFR Chapter XII
5. Information and assistance. Guidance on electronic records management and related issues may be obtained from:

TC 90-1 Attachment

FIRMR Bulletin B-1

- a. General Services Administration
Regulations Analysis Division (KMR)
18th and F Streets, NW
Washington, DC 20405

Telephone Commercial or FTS (202) 501-3194

- b. National Archives and Records Administration
Agency Services Division (NIA)
7th Street and Pennsylvania Ave, NW
Washington, DC 20408

Telephone FTS or (202) 724-1453

6. Definitions.

"Data base" means a set of data, consisting of at least one data file, that is sufficient for a given purpose.

"Data base management system" means a software system used to access and retrieve data stored in a data base.

"Data file" means related numeric, textual, or graphic information that is organized in a strictly prescribed form and format.

"Electronic record" means any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 USC 3301. Electronic records include numeric, graphic and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks. Unless otherwise noted, these requirements apply to all electronic records systems, whether on microcomputers, minicomputers, or main-frame computers, regardless of storage media, in network or stand-alone configurations.

"Electronic records system" means any information system that produces, manipulates, or stores Federal records by using a computer.

"Information system" has the meaning given to it by the Office of Management and Budget in Circular No. A-130: "...the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual."

FIRMR Bulletin B-1

"Text documents" means narrative or tabular documents, such as letters, memorandums, and reports, in loosely prescribed form and format.

7. Acronyms.

NARA National Archives and Records Administration
NIST National Institute of Standards and Technology
GAO General Accounting Office
OMB Office of Management and Budget

8. Agency responsibilities. The head of each Federal agency should:

a. Assign responsibility to develop and implement an agencywide program for the management of all records created, received, maintained, used, or stored on electronic media; and notify the following organizations of the name and title of the person assigned the responsibility:

- (1) General Services Administration
Regulations Analysis Division (KMR)
Washington, DC 20405
- (2) National Archives and Records Administration
Office of Records Administration (NI)
Washington, DC 20408

b. Integrate the management of electronic records with other records and information resources management programs of the agency.

c. Incorporate electronic records management objectives, responsibilities, and authorities in pertinent agency directives and disseminate them throughout the agency as appropriate.

d. Establish procedures for addressing records management requirements, including recordkeeping and disposition requirements, before approving new electronic records systems or enhancements to existing systems.

e. Ensure that adequate training is provided for users of electronic records systems in the operation, care, and handling of the equipment, software, and media used in the system.

f. Develop and maintain up-to-date documentation about all electronic records systems that is adequate to: specify all technical characteristics necessary for reading or processing the

FIRMR Bulletin B-1

records; identify all defined inputs and outputs of the system; define the contents of the files and records; determine restrictions on access and use; understand the purposes and functions of the system; describe update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and ensure the timely, authorized disposition of the records.

g. Specify the location, manner, and media in which electronic records will be maintained to meet operational and archival requirements, and maintain inventories of electronic records systems to facilitate disposition.

h. Develop and secure NARA approval of records disposition schedules, and ensure implementation of their provisions.

i. Specify the methods of implementing controls over national security-classified, sensitive, proprietary, and Privacy Act records stored and used electronically.

j. Establish procedures to ensure that the guidelines of this bulletin are applied to those electronic records that are created or maintained by contractors.

k. Ensure compliance with applicable Governmentwide policies, procedures, and standards such as those issued by OMB, GAO, GSA, NARA and NIST.

l. Review electronic records systems periodically for conformance to established agency procedures, standards, and policies as part of the periodic reviews required by 44 U.S.C. 3506. The review should determine if the records have been properly identified and described, and whether the schedule descriptions and retention periods reflect the current informational content and use. If not, or if substantive changes have been made in the structure, design, codes, purposes, or uses of the system, submit an SF 115, Request for Records Disposition Authority, to NARA at the address shown in 8.a. above.

9. Creation and use of data files.

a. For electronic records systems, disposition instructions for the data should be incorporated into the system's design.

b. Agencies should maintain adequate and up-to-date technical documentation for each electronic records system. The minimum documentation required is a narrative description of the system; physical and technical characteristics of the records, including a record layout that describes each field including its

FIRMR Bulletin B-1

name, size, starting or relative position, and a description of the form of the data (such as alphabetic, zoned decimal, packed decimal, or numeric), or a data dictionary or the equivalent information associated with a data base management system including a description of the relationship between data elements in data bases; and any other technical information needed to read or process the records.

10. Creation and use of text documents.

a. Electronic records systems that maintain the official file copy of text documents on electronic media should meet the following minimum requirements:

- (1) Provide a method, such as an indexing or text search system, for all authorized users of the system to retrieve desired documents;
- (2) Provide an appropriate level of security to ensure integrity of the documents;
- (3) Provide a standard interchange format when necessary to permit the exchange of documents on electronic media between agency computers using different software/operating systems and the conversion or migration of documents on electronic media from one system to another; and
- (4) Provide for the disposition of the documents including the requirements for transferring permanent records to NARA (see 36 CFR 1228.188).

b. Before a document is created electronically on electronic records systems that will maintain the official file copy on electronic media, each document should be identified sufficiently to enable authorized personnel to retrieve, protect and carry out the disposition of documents in the system. Appropriate identifying information for each document maintained on the electronic media may include: office of origin, file code, key words for retrieval, addressee (if any), signator, author, date, authorized disposition (coded or otherwise), and security classification (if applicable). Agencies should ensure that records maintained on such systems can be correlated with related records on paper, microform, or other media.

11. Judicial use of electronic records. Electronic records may be admitted in evidence to Federal courts for use in court proceedings (Federal Rules of Evidence 803(8)) if trustworthiness is established by thoroughly documenting the recordkeeping system's operation and the controls imposed upon it. Agencies

FIRMR Bulletin B-1

should implement the following procedures to enhance the legal admissibility of electronic records:

- a. Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.
- b. Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure system protection against such problems as power interruptions.
- c. Identify the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage media, and the NARA-approved disposition of all records.
- d. Coordinate all of the above with legal counsel and senior IRM and records management staff.

12. Security of electronic records. Agencies should implement and maintain an effective records security program that incorporates the following:

- a. Ensures that only authorized personnel have access to electronic records.
- b. Provides for back up and recovery of records to protect against information loss.
- c. Ensures that appropriate agency personnel are trained to safeguard sensitive or classified electronic records.
- d. Minimizes the risk of unauthorized alteration or erasure of electronic records.
- e. Ensures that electronic records security is included in computer systems security plans prepared pursuant to the Computer Security Act of 1987 (40 USC 759).

13. Selection and maintenance of electronic records storage media.

a. Agencies should select appropriate media and systems for storing agency records throughout their life cycle, which meet the following requirements:

- (1) Permit easy retrieval in a timely fashion;

FIRMR Bulletin B-1

(2) Facilitate distinction between record and nonrecord material;

(3) Retain the records in a usable format until their authorized disposition date; and

(4) When appropriate, meet requirements for transferring permanent records to NARA (see 36 CFR 1228.188).

b. The following factors should be considered before selecting a storage medium or converting from one medium to another:

(1) The authorized life of the records, as determined during the scheduling process;

(2) The maintenance necessary to retain the records;

(3) The cost of storing and retrieving the records;

(4) The records density;

(5) The access time to retrieve stored records;

(6) The portability of the medium (that is, selecting a medium that will run on equipment offered by multiple manufacturers) and the ability to transfer the information from one medium to another (such as from optical disk to magnetic tape); and

(7) Whether the medium meets the current applicable Federal Information Processing Standards.

c. Agencies should avoid the use of floppy disks for the exclusive long-term storage of permanent or unscheduled electronic records.

d. Agencies should ensure that all authorized users can identify and retrieve the information stored on diskettes, removable disks, or tapes by establishing or adopting procedures for external labeling.

e. Agencies should ensure that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the agency's current hardware and software. Before conversion to a different medium, agencies must determine that the authorized disposition of the electronic records can be implemented after conversion.

FIRMR Bulletin B-1

f. Agencies should back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records should be maintained in storage areas separate from the location of the records that have been copied.

g. Maintenance of magnetic computer tape.

(1) Agencies should test magnetic computer tapes no more than 6 months prior to using them to store electronic records that are unscheduled or scheduled for permanent retention. This test should verify that the tape is free of permanent errors and in compliance with NIST or industry standards.

(2) Agencies should maintain the storage and test areas for computer magnetic tapes containing permanent and unscheduled records at the following temperatures and relative humidities:
Constant temperature - 62 to 68 degrees F.
Constant relative humidity - 35% to 45%.

(3) Agencies should rewind under controlled tension all tapes containing unscheduled and permanent records every 42 months.

(4) Agencies should annually read a statistical sample of all reels of magnetic computer tape containing permanent and unscheduled records to identify any loss of data and to discover and correct the causes of data loss. In tape libraries with 1800 or fewer reels, a 20% sample or a sample size of 50 reels, whichever is larger, should be read. In tape libraries with more than 1800 reels, a sample of 384 reels should be read. Tapes with 10 or more errors should be replaced and, when possible, lost data should be restored. All other tapes which might have been affected by the same cause (i.e., poor quality tape, high usage, poor environment, improper handling) should be read and corrected as appropriate.

(5) Agencies should copy permanent or unscheduled data on magnetic tapes before the tapes are 10 years old onto tested and verified new tapes.

(6) External labels (or the equivalent automated tape management system) for magnetic tapes used to store permanent or unscheduled electronic records should provide unique identification for each reel, including the name of the organizational unit responsible for the data, system title, and security classification, if applicable. Additionally, the

FIRMR Bulletin B-1

following information should be maintained for (but not necessarily attached to) each reel used to store permanent or unscheduled electronic records: file title(s); dates of creation; dates of coverage; the recording density; type of internal labels; volume serial number, if applicable; number of tracks; character code/software dependency; information about block size; and reel sequence number, if the file is part of a multi-reel set. For numeric data files, include record format and logical record length, if applicable; data set name(s) and sequence, if applicable; and number of records for each data set.

(7) Agencies should prohibit smoking and eating in magnetic computer tape storage libraries and test or evaluation areas that contain permanent or unscheduled records.

h. Maintenance of direct access storage devices.

(1) Agencies should issue written procedures for the care and handling of direct access storage devices which draw upon the recommendations of the manufacturers.

(2) External labels for diskettes or removable disks used when processing or temporarily storing permanent or unscheduled records should include the following information: name of the organizational unit responsible for the records; descriptive title of the contents; dates of creation; security classification, if applicable; and identification of the software and hardware used.

14. Retention of electronic records. Agencies should establish policies and procedures to ensure that electronic records and their documentation are retained as long as needed by the Government. These retention procedures should include provisions for:

a. Scheduling the disposition of all electronic records, as well as related documentation and indexes, by applying General Records Schedules (particularly GRS 20 or 23) as appropriate or submitting an SF 115, Request for Records Disposition Authority, to NARA (see 36 CFR 1228). The information in electronic records systems, including those operated for the Government by a contractor, should be scheduled as soon as possible but no later than one year after implementation of the system.

b. Transferring a copy of the electronic records and any related documentation and indexes to the National Archives at the time specified in the records disposition schedule in accordance with instructions found in 36 CFR 1228.188. Transfer may take

FIRMR Bulletin B-1

place at an earlier date if convenient for both the agency and the NARA.

- c. Establishing procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorized life cycle.

15. Destruction of electronic records. Electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules. At a minimum, each agency should ensure that:

- a. Electronic records scheduled for destruction are disposed of in a manner that ensures protection of any sensitive, proprietary, or national security information.

- b. Magnetic recording media previously used for electronic records containing sensitive, proprietary, or national security information are not reused if the previously recorded information can be compromised by reuse in any way.

Thomas J. Buckholtz
Commissioner
Information Resources
Management Service

FIRMR Bulletin B-1
Attachment A

COMPARISON OF VARIOUS MEDIA FOR INFORMATION STORAGE AND RETRIEVAL

Feature	Medium				
	Paper	Microform	Magnetic Tape	Magnetic Diskette	Optical disk (read only)
Life expectancy.	Very Good	Very Good	Good	Good	Mfgs. claims are 10 years.

If paper quality, ink and storage conditions are good (70-100 years).

If microform properly processed and stored.
(Silver - 100s of years.)
(Diaz and vesicular - 100 years).

Magnetic tape is subject to equipment malfunction or magnetic erasure (10-12 years with periodic exercising).

Magnetic Diskettes are subject to equipment malfunction or magnetic erasure (10-15 years).

Acceptable for transfer of permanent records to NARA?	Yes	Yes, if silver gelatin.	Yes	No	No
---	-----	-------------------------	-----	----	----

Special equipment required to read?	No	Yes, for normal operation. Simple optics will suffice in emergencies.	Yes	Yes	Yes
-------------------------------------	----	---	-----	-----	-----

Data easy to alter unnoticed?	No	No	Yes	Yes	No
-------------------------------	----	----	-----	-----	----

COMPARISON OF VARIOUS MEDIA FOR INFORMATION STORAGE AND RETRIEVAL

Feature	Medium				
	Paper	Microform	Magnetic Tape	Magnetic Diskette	Optical disk (read only)
Data may be easily accidentally destroyed.	No	No	Yes	Yes	No
Complex indexing easily accomplished?	No	No (Yes, if computer assisted retrieval system is used).	Yes	Yes	Yes
		With special software.		With special software.	
				With special software.	
Data easy to retrieve?	Volume Small-Yes upon Large-No	Depends upon indexing and labeling scheme. Computer assisted retrieval very helpful for large collections.	Yes, if properly indexed.	Yes, if properly indexed.	Yes, if properly indexed.
Data easy to electronically process after retrieval?	No	No	Yes	Yes readable-Yes Raster scan -No	Machine

